

RFC 2350 TTIS RS PMI BOGOR

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi TTIS RS PMI BOGOR berdasarkan RFC 2350, yaitu informasi dasar mengenai TTIS RS PMI BOGOR, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi TTIS RS PMI BOGOR.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 25 Mei 2026.

1.2. Daftar Distribusi untuk Pemberitahuan

Pemberitahuan mengenai perubahan atau pembaruan dokumen RFC 2350 akan diinformasikan kepada konstituen TTIS RSPMI Bogor:

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
<https://rspmibogor.or.id/> (versi Bahasa Indonesia)

1.4 Keaslian Dokumen

Dokumen ini adalah dokumen asli yang telah ditandatangani secara sah oleh Ketua Tim TTI RS PMI Bogor.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 TTIS RS PMI BOGOR;
Versi	: 1.0;
Tanggal Publikasi	: 08 Oktober 2026;
Kedaluwarsa	: 07 Oktober 2029 atau "Dokumen ini valid hingga dokumen terbaru dipublikasikan."

2. Informasi Data/Kontak

2.1. Nama Tim

Kepanjangan dari TIM TANGGAP INSIDEN SIBER (COMPUTER SECURITY INCIDENT RESPONSE TEAM-CSIRT)
Disingkat : TTIS RS PMI BOGOR.

2.2. Alamat

Jl. Raya Pajajaran No.80, RT.02/RW.05, Tegallega, Kecamatan Bogor Tengah, Kota Bogor, Jawa Barat 16153

2.3. Zona Waktu

Bogor (GMT+07:00)

2.4. Nomor Telepon

+62 251 8324080

2.5. Nomor Fax

+62 251 8324709

2.6. Telekomunikasi Lain

+62 813-8678-8389

2.7. Alamat Surat Elektronik (*E-mail*)

ttis.rspmibogor@rspmibogor.id

2.8. Kunci Publik (*Public Key*) dan Informasi/Data PGB dari email pada subbab 2.7

Bits : 3072 bit

ID : 864C56003A509F94

Key Fingerprint : 0F61 3988 1163 9624 8B56 1F03 864C 5600 3A50 9F94

-----BEGIN PGP PUBLIC KEY BLOCK-----

xsDNBGrH DU8BDAC1mYgVbZVzMiWouobJhmGpr+pqFfnAB1Uczs4hfarLR43YFJYX
BZ2UeZf19xFoJSJLuqAoSrcueMOsqoBGxzvK6SuT2Y5U28r+s0yzOyhpW7WDI9JR
EN6hmqA9+FL1k2hzY82mb56TNLkDD44lx89t2kBC7ceN32NS9P16vvkbLbA7nVh0
Hljdsd7ugqw/0U9aiOQYDLX5Cm/+uKwMKjtu8Dj13N6MqBHOqCE15psCMWFUiT69U
fy6JH3fHwE5lprAlrOrMYZPSvL5qJf82elwzFChJlq28HqgXkY0X8uMzJV1ekFS
PmTjGIJjw6LmPk6zAfDMA1BkB+QvuQTZSqOx4MIO5bVVDg8UECNmENUyTC7zynPT
Lp5oN9IyAwJC/SC8HSfTsUVIbTILE9t2z+OxLwDbbyJz9yfORg+fC5MDs9MKmkZ9
eRYoeN1kDAdBVmPLngAnrXlviGRESbwEVhWOBhvX55GSwTMVF9ca9BhEKSBBAYVBW
GIJYcAUhshCJjeUAEQEAAC0wVFRJU19SU1BNSV9CT0dPUiA8dHRpcy5yc3BtaWJv
Z29yQHJzcG1pYm9nb3luaWQ+wsENBBMBCAA3FiEED2E5iBFjliSLVh8DhkwWADpQ
n5QFAmrHDVAFcQWjmoACGwMECwkIBwUVCakKCwUWAgMBAAAKCRCGTFYA0ICfIC
IZ

DACVG9cy/SXTwPmYg5x97dTcy+S30t2BpiYKWZK/b94YVpBE+vDOF5MIOT4AEIHS
3R7s2VcreU1d3b3ns7hzVv5jepXoJfrlqk/hhkNWCZtA93VIdHK5PRV8liHqTSYt
vxK+Swef9n2xZlIPJ5JBfDBbxSuo/n9QibO1o9apvEJn/+ai6ppHEGb19wWdDATi
Bfc11KaGh5AV5YfYFPCWmZKK2/1h/cCE464B6Arqlhtpc87q11Ftxaxa1Sb0LITy
tS70qf2OLC/hM9GLG45YxhbLnKkTWgDIIncwXd6Ykq44qUIA+K+F412ghvahWz83
7CBJ18VmbvWLXLYIScCIF0IDudGdmk7oH94UxBwAhVUGbkqrlsByz3PMJOE+bg3E
Uru4sOILf9klpwr/rJql2pj82qqYiyKQ61IMlpjq5SIOXi3V95JmguKqXYCLdpX8
WrKHC7gJF1zo/55Ddih9ZXZwWUjprs4YapTKz4KDXvd5PpRcsDKb2NESMYpJuMSO
GcvOwM0EascNUAEMANfA9jOplezOh0M5S8PzdIOZbj1tu6vlqoNaGH9qS8wAeoXh
PlnM6F17eDRGLPCM2H6H1FBZCcW83RDzgdFwGTv+PaMorC1tvYuXExXUtP8kz/Xh
Y1GQAvA5JhC/+12g5lpAlBmE5PHA77X6e2yTtDSAN19hOY/mvJPKTmyN39pN9As7
4e/O5PkXHI+1yiPR3vNck4586NJM4Z4Co62TWss881AsjnW8DTHxxG494ltxz82R
0gflaSP6LPaGvon85n5nex9XS/SvT35fS9O0IL47G35oupW7J7sTkTCYOIhcnHxr
3tkKBbwIzalfsaEg5MmlhYM5WYg3com3DUS54q0uiQVnup6E8sLEZ23Wv4eW6s1e

RHZSdQjsBW5M4StelylHpFfNnoRx9VJ/l6hNpdPuvwt5FwO5Dd+LTztQRRR35iMa
cuMr4zexQY6DniF9uqerhvFsGJvsVBLcyUbvz2hOcl8XRJZX/56+ioSqQkcuqih
O/Jsqj1ux188M+osiQARAQABwsD8BBgBCAAmFiEED2E5iBFjliSLVh8DhKxWADpQ
n5QFAmrHDVEFCQWjmoACGwwACGkQhKxWADpQn5TdvQv/YY8Ui9/qDKV86EWcV14
i2rqRDIImXEbi+4UrCG8d6DbzZZH3ZjZY+bgETu0ALVkaqXV2KglwXP7wl8i9rNZP
nTSo+HK/UtZECaxgvAKRuVPN+1u0u7dZsPEnjwnog09T3wuxlL4cCNjlvSAzV+7
H99eJixexvMYvRG66MvNyadjES64W5K+cxgeEb/mccQiyzCUPQuJoFbxZpSCLQY8
n7A7RRDirwbeiCMtNETiRpM/YwM8aWmW0Um+qSD+HoN41ylcTHmOLGz3fVPwdlck
QbRkZKnAXRHy2iUMHpbFtTQ4P/NBEy1Uet+rHtqlyWF2INYH993xv/khVJuV3CI0
7mWUgtMpBtCbDsg6lnAoP/yrwsjGiw6LJOsnejTz+WOYk924vEO4epl+eV3snnXs
tF16NBv+fg47vFcmvG5cTFIFpzJZQGFrs7I9HFjkRJWCXBielicB0q688aleRie
W+5uQpZFSceL0GN4i6/4BHjUfrlu8pvEv8EI1i4Rr+vc
=v/gH
-----END PGP PUBLIC KEY BLOCK-----

2.9. Anggota Tim

Susunan Anggota TTIS RS PMI Bogor sesuai dengan keputusan Direktur Utama Nomor : I.0098/KTPS-RSPMI/V/2026 Tentang : TIM TANGGAP INSIDEN SIBER (*COMPUTER SECURITY INCIDENT RESPONSE TEAM-CSIRT*)

2.10. Informasi/Data lain

-

2.11. Catatan-catatan pada Kontak TTIS RS PMI BOGOR

Dapat disesuaikan terkait kontak dari operasional TTIS.

3. Mengenai TTIS RS PMI BOGOR

3.1. Visi

Visi TTIS RS PMI BOGOR adalah Mewujudkan penanganan insiden keamanan siber yang efektif, cepat, terkoordinasi, dan berkesinambungan guna mendukung keamanan dan keberlangsungan layanan informasi serta sistem elektronik di lingkungan RS PMI Bogor.

3.2. Misi

Menyelenggarakan penanganan dan penanggulangan insiden keamanan siber secara cepat, tepat, terkoordinasi, dan berkesinambungan guna menjaga keamanan, kerahasiaan, integritas, dan ketersediaan informasi serta sistem elektronik di lingkungan RS PMI Bogor.

3.3. Konstituen

Seluruh unit kerja dan pengguna sistem elektronik di lingkungan RS PMI Bogor.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan TTIS RS PMI BOGOR bersumber dari Anggaran RS PMI Bogor sesuai dengan kebijakan dan ketentuan pengelolaan anggaran yang berlaku.

TTIS RS PMI Bogor berada dalam struktur organisasi dan tata kelola RS PMI Bogor serta dapat melakukan koordinasi dengan Badan Siber dan Sandi Negara (BSSN) dan pihak terkait lainnya dalam rangka penanganan insiden keamanan siber sesuai dengan kewenangan dan ketentuan yang berlaku.

3.5. Otoritas

TTIS RS PMI Bogor menerima mandat dari manajemen RS PMI Bogor untuk melaksanakan penanganan insiden keamanan siber yang terjadi pada sistem elektronik dan layanan informasi dalam lingkup RS PMI Bogor.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/Level Dukungan

TTIS RS PMI BOGOR melayani penanganan insiden siber dengan jenis berikut :

- a. Malware, virus, ransomware, trojan, spyware, dan perangkat lunak berbahaya lainnya;*
- b. Phishing, social engineering, dan pencurian kredensial;*
- c. Akses tidak sah terhadap sistem elektronik, aplikasi, jaringan, atau akun pengguna;*
- d. Kebocoran atau indikasi kompromi informasi dan data;*
- e. Serangan terhadap jaringan dan sistem elektronik;*
- f. Gangguan terhadap ketersediaan layanan sistem elektronik;*
- g. Eksploitasi kerentanan pada aplikasi, sistem, perangkat, atau jaringan;*
- h. Insiden keamanan pada perangkat endpoint/server;*
- i. Insiden keamanan informasi lainnya yang berdampak atau berpotensi berdampak terhadap layanan RS PMI Bogor.*

Tingkat dukungan

TTIS memberikan dukungan berdasarkan tingkat dampak dan urgensi insiden, antara lain:

Level Tinggi

Insiden yang berdampak signifikan terhadap keamanan informasi, sistem elektronik, atau keberlangsungan layanan rumah sakit dan memerlukan penanganan serta koordinasi segera.

Level Sedang

Insiden yang berdampak terhadap sebagian sistem atau unit kerja dan memerlukan penanganan terkoordinasi.

Level Rendah

Insiden atau indikasi keamanan yang memiliki dampak terbatas dan dapat ditangani melalui prosedur penanganan rutin.

Penentuan tingkat insiden dilakukan berdasarkan hasil identifikasi, analisis, dan triage oleh TTIS dengan mempertimbangkan dampak terhadap kerahasiaan, integritas, ketersediaan, dan keberlangsungan layanan.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

TTIS RS PMI Bogor melakukan kerja sama dan koordinasi dengan unit kerja internal serta pihak eksternal yang berkepentingan dalam penanganan insiden keamanan siber.

Kerja sama dapat dilakukan dengan:

unit kerja terkait di RS PMI Bogor;
pengelola sistem/aplikasi;
penyedia layanan teknologi informasi;
CSIRT organisasi/sektoral lainnya;
Health-CSIRT (Kementrian Kesehatan);
Nat-CSIRT (BSSN); dan
pihak berwenang lainnya sesuai kebutuhan dan ketentuan yang berlaku.

Informasi mengenai insiden keamanan siber dikelola berdasarkan prinsip kerahasiaan, integritas, dan kebutuhan untuk mengetahui (need-to-know).

Informasi yang bersifat terbatas, sensitif, atau mengandung data yang dilindungi tidak akan disebarluaskan kepada pihak yang tidak berwenang. Pengungkapan informasi kepada pihak lain dilakukan berdasarkan kewenangan, kebutuhan penanganan insiden, persetujuan pihak berwenang, dan ketentuan peraturan perundang-undangan yang berlaku.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi umum, TTIS RS PMI Bogor dapat menggunakan:

surat elektronik resmi;
telepon resmi;
komunikasi internal RS PMI Bogor; dan
media komunikasi resmi lainnya yang ditetapkan.

Untuk komunikasi yang mengandung informasi terbatas atau sensitif, TTIS RS PMI Bogor menggunakan mekanisme komunikasi terenkripsi berbasis kunci PGP

dan/atau autentikasi yang sesuai dengan tingkat sensitivitas informasi serta kebijakan keamanan yang berlaku.

5. Layanan

5.1. Layanan

Layanan yang diberikan oleh TTIS RS PMI BOGOR yaitu :

5.1.1. Penanggulangan Dan Pemulihan Insiden Siber

TTIS RS PMI Bogor memberikan layanan penanggulangan dan pemulihan insiden keamanan siber melalui kegiatan penerimaan laporan, identifikasi, analisis, triage, koordinasi penanganan, mitigasi, pemulihan, serta evaluasi pascainsiden.

Penanganan dilakukan dengan mempertimbangkan tingkat dampak insiden terhadap sistem informasi, keamanan informasi, dan keberlangsungan pelayanan RS PMI Bogor.

5.1.2. Penyampaian Informasi Insiden Siber Kepada Pihak Terkait

TTIS menyampaikan informasi mengenai insiden keamanan siber kepada pihak internal maupun eksternal yang berkepentingan sesuai dengan kewenangan dan kebutuhan penanganan insiden.

Informasi yang disampaikan dapat mencakup:

- jenis dan status insiden;
- sistem atau layanan yang terdampak;
- dampak insiden;
- tindakan penanganan yang telah dilakukan;
- rekomendasi mitigasi; dan
- informasi lain yang diperlukan untuk penanganan insiden.

5.1.3. Diseminasi Informasi Untuk Mencegah dan/atau Mengurangi Dampak dari Insiden Siber

TTIS melakukan penyebaran informasi keamanan siber kepada konstituen untuk meningkatkan kesiapsiagaan dan mengurangi risiko insiden.

Informasi dapat berupa:

- peringatan keamanan;
- informasi mengenai ancaman yang sedang berkembang;
- rekomendasi mitigasi;
- panduan penanganan insiden;
- himbauan keamanan siber; dan
- materi peningkatan kesadaran keamanan informasi.

5.2. Fungsi

TTIS RS PMI BOGOR memiliki fungsi-fungsi dalam menjalankan layanannya, antara lain :

5.2.1. Fungsi Utama

Fungsi utama yang diberikan TTIS RS PMI BOGOR yaitu :

5.2.1.1. Pemberian Peringatan Terkait Keamanan Siber

TTIS memberikan peringatan kepada konstituen mengenai ancaman, kerentanan, atau kejadian keamanan siber yang dapat berdampak terhadap sistem elektronik dan layanan RS PMI Bogor.

5.2.1.2. Perumusan Panduan Teknis Penanganan Insiden Siber

TTIS menyusun dan/atau memberikan rekomendasi panduan teknis penanganan insiden keamanan siber sebagai acuan bagi unit kerja dalam melakukan pencegahan, mitigasi, penanganan, dan pemulihan insiden.

5.2.1.3. Pencatatan Setiap Laporan/Aduan Yang Dilaporkan, Pemberian Rekomendasi Langkah Penanganan Awal Kepada Pihak Terdampak

TTIS menerima dan mencatat laporan insiden keamanan siber yang diterima melalui kanal resmi.

Setiap laporan dianalisis untuk menentukan tindakan awal yang diperlukan dan memberikan rekomendasi kepada pihak terdampak sesuai dengan jenis dan tingkat insiden.

5.2.1.4. Pemilahan (Triage) Insiden Siber Sesuai Dengan Kriteria yang Ditetapkan Dalam Rangka Memprioritaskan Insiden Siber yang Akan Ditangani

TTIS melakukan triage terhadap setiap laporan berdasarkan jenis insiden, tingkat dampak, urgensi, sistem yang terdampak, serta potensi gangguan terhadap keamanan informasi dan keberlangsungan layanan rumah sakit.

Hasil triage digunakan untuk menentukan prioritas dan metode penanganan insiden.

5.2.1.5. Penyelenggaraan Koordinasi Penanganan Insiden Siber Kepada Pihak yang Berkepentingan

TTIS melakukan koordinasi dengan unit kerja yang terdampak, pimpinan, pengelola sistem, penyedia layanan, maupun pihak eksternal yang berwenang apabila diperlukan.

Koordinasi dilakukan untuk memastikan penanganan insiden berjalan secara terarah dan terdokumentasi.

5.2.1.6. Penyelenggaraan Fungsi Lainnya Sesuai Kebutuhan

TTIS dapat melaksanakan fungsi lain yang berkaitan dengan keamanan siber sesuai kebutuhan organisasi, kebijakan RS PMI Bogor, kompetensi personel, serta kewenangan yang diberikan melalui dokumen legal pembentukan TTIS.

5.2.2. Fungsi Tambahan (Lainnya)

Fungsi tambahan yang diberikan oleh TTIS RS PMI BOGOR yaitu :

5.2.2.1. Penanganan Kerawanan Sistem Elektronik

TTIS melakukan koordinasi dalam identifikasi, penilaian, dan penanganan kerawanan sistem elektronik yang dapat dimanfaatkan untuk melakukan serangan atau mengganggu keamanan sistem.

5.2.2.2. Penanganan Artefak Digital

TTIS melakukan pengumpulan, dokumentasi, pengamanan, dan analisis awal artefak digital yang berkaitan dengan insiden keamanan siber sesuai kewenangan dan prosedur yang berlaku.

5.2.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

TTIS menyampaikan informasi mengenai hasil pengamatan terhadap potensi ancaman keamanan siber yang relevan kepada unit atau pihak yang berkepentingan sebagai bahan mitigasi.

5.2.2.4. Pendeteksian Serangan

TTIS melakukan atau mengoordinasikan pendeteksian terhadap indikasi serangan keamanan siber melalui pemantauan, analisis log, laporan pengguna, sistem keamanan, maupun sumber informasi lain yang tersedia.

5.2.2.5. Analisis Risiko Keamanan Siber

TTIS memberikan dukungan dalam identifikasi dan analisis risiko keamanan siber yang berkaitan dengan sistem elektronik dan layanan informasi RS PMI Bogor serta memberikan rekomendasi mitigasi sesuai kebutuhan.

5.2.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

TTIS memberikan konsultasi kepada unit kerja terkait mengenai kesiapan menghadapi insiden keamanan siber, termasuk kesiapan prosedur, sumber daya, komunikasi, pencadangan, pemulihan, dan aspek teknis lainnya.

5.2.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

TTIS mendukung peningkatan kesadaran dan kepedulian keamanan siber melalui edukasi, sosialisasi, penyampaian informasi, simulasi, kampanye keamanan informasi, dan kegiatan peningkatan kompetensi yang relevan bagi pengguna sistem elektronik di lingkungan RS PMI Bogor.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke ttis.rspmibogor@rspmibogor.id dengan melampirkan sekurang-kurangnya :

- a. Identitas dan informasi kontak pelapor;
- b. Kronologi singkat kejadian;
- c. Waktu terjadinya atau diketahuinya insiden;
- d. Sistem, aplikasi, perangkat, atau layanan yang terdampak;
- e. Bukti insiden berupa foto, screenshot, log file, atau artefak digital yang relevan; dan
- f. Informasi pendukung lain yang diperlukan untuk proses identifikasi dan penanganan insiden.

TTIS dapat meminta informasi tambahan apabila diperlukan untuk proses verifikasi, analisis, dan penanganan insiden.

7. Disclaimer

TTIS RS PMI Bogor berupaya memberikan layanan penanganan insiden keamanan siber sesuai dengan kewenangan, sumber daya, prosedur, dan kemampuan teknis yang tersedia.

Informasi, rekomendasi, dan panduan yang diberikan oleh TTIS ditujukan untuk mendukung upaya penanganan dan mitigasi insiden keamanan siber. Pelaksanaan tindakan pada sistem elektronik tetap dilakukan oleh pihak yang memiliki kewenangan terhadap sistem tersebut sesuai dengan kebijakan dan prosedur RS PMI Bogor.

TTIS RS PMI Bogor menjaga kerahasiaan informasi yang diperoleh selama proses penanganan insiden dan hanya melakukan pengungkapan informasi kepada pihak yang berwenang atau berkepentingan sesuai dengan ketentuan yang berlaku.